SECRET

(b)(1)
(b)(3)

Organizational Innovation

An Interview with TTIC Director John Brennan

66

A National Counterterrorism Center ... will build upon the concept of TTIC and allow further integration of US government counterterrorism capabilities.

99

Editor's Note: John Brennan was named director of the Terrorist Threat Integration Center (TTIC) on 12 March 2003. After joining the Central Intelligence Agency in 1980, he served in a variety of analytic and management positions focusing primarily on the Middle East and terrorism. He was a daily intelligence briefer at the White House in the mid-1990s and then served as _____

_____ *Mr. Brennan is a graduate of Fordham University and earned an MA from the University of Texas.* _____

Mr. Brennan was interviewed on 21 July 2004 by _____ _____ *of the* Studies in Intelligence *Editorial Board. Subsequent to the interview, the TTIC director reflected on the recently proposed National Counterterrorism Center, telling* Studies: *"I am a strong proponent of a National Counterterrorism Center, as it will build upon the concept of TTIC and allow further integration of*

US government counterterrorism capabilities. The design, mission, and responsibilities of such a center need to be carefully thought through, however, as we must find a construct that optimizes those capabilities without disrupting the very important and critical work that is underway throughout the government. The center's mission **must** *be clearly defined and its structure well engineered if it is to realize its potential."* _____

On 27 October, Mr. Brennan was appointed as the (interim) director of the National Counterterrorism Center. He will continue to serve as the director of TTIC until its functions are absorbed by the new national center. _____

As with all Studies in Intelligence *articles, the statements, assertions, and opinions expressed in this article are those of the interview participants alone and do not necessarily reflect official positions or views of any US government entity.* _____

*   *   *

John, the Terrorist Threat Integration Center was established in 2003 by order of the president, and you've recently consolidated your staff here at the new _____ _____ *facility. Looking back, what are the criteria by which you, as the director, believe the effectiveness of TTIC should be assessed after its first year of existence? What should the cate-*

UNCLASSIFIED//FOUO

SECRET

1

~~SECRET~~
TTIC

> ## 66
> ## TTIC has access to 26 networks, classified and unclassified, an unprecedented breadth of access within the US government.
> ## 99

gories on the report card be, and what kind of grades would you award the center against these criteria?

Well, I think that the report card would be diverse because TTIC has such diverse responsibilities. First of all, we were charged by the president to make sure that there is one place in the US government that has access to all of the information that is available to the government that is related to the terrorist threat. And I think, looking back over the past year, we have been successful in terms of bringing all of those different networks into TTIC. Right now, we have access to 26 networks, classified and unclassified, an unprecedented breadth of access within the US government on terrorism-related matters. We are soon going to expand to 28 networks, so the first metric, I think, should be the extent of improved, shared access to information, and I think we get a pretty good grade there. And our grade should reflect positively on the partner agencies that have been willing to provide us this unfettered and unrestricted access.

Secondly, it's not sufficient just to have access to all these networks; you have to be able to take advantage and leverage that access. And so we are now moving forward on having an integrated architecture within TTIC so that those networks can be brought together to enable us to conduct federated searches against them. By the end of this month, we will have, for the first time, databases from different networks pulled together so that we can do a federated search against them. Through the rest of the year, we are going to be adding networks onto that integrated architecture so that the analysts and others can do these federated searches, because a simultaneous search against multiple networks is much more powerful than sequential searches against individual networks. So, since we are not there yet, I would give us a very tentative grade there of "in progress;" we seem to be on track, we are not there yet, but we certainly have the design ready to go.

Another of our responsibilities is to make sure that we are able to disseminate information and analysis to all of the appropriate federal consumers. Here I think we get a pretty good grade; I'll give us something in the B-plus category. We now have two principal mechanisms to get information out electronically, which I think really is the way we need to go as far as making sure there's timely dissemination.
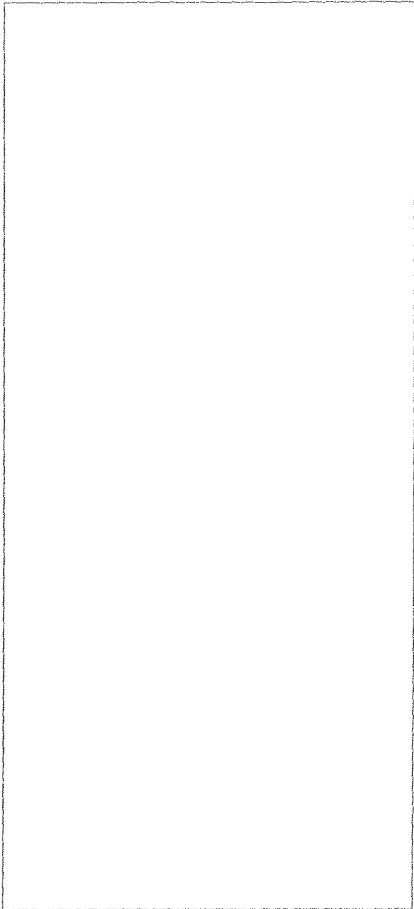
One of the areas that we are still "growing" is actually doing the analysis. We have, quite honestly, precious few analysts; there are a couple dozen analysts who are doing all-source analysis. And we are really looking forward to additional analysts coming in from our partner agencies. We do a good job as far as reportorial coverage, but as far as the in-depth, strategic pieces that really provide insights and understanding to the customers about the nature of the terrorist threat, we're not there yet.

66
I see terrorism analysis as a distinct discipline in the intelligence arena.
99

That's a good segue for discussing the challenges you face regarding staffing and subject matter expertise. With respect to the infusion of new analysts that you are receiving into TTIC from various agencies, what portion of them arrives with subject matter expertise on terrorism? Are most expected to learn on the job, and do you envision a training program of sorts in TTIC to supplement on-the-job training?

Well it's a little bit of all of the above. Most of the analysts who come to TTIC have some established area of expertise. Sometimes it's in the terrorism area, and sometimes it's in areas that are very much related to terrorism. They could be analysts of those countries that play an important role in terrorism. They may come with background related to potential targets of terrorist attacks. So they have relevant experience. What we are trying to do here in TTIC is to develop a whole analytic cadre of different backgrounds and expertise so we can leverage their expertise.

We have to develop our own training programs and training classes, but we are really looking to those partner agencies to provide analysts who are already trained in intelligence and have a background in terrorism. We recognize that a lot of these agencies are strapped as far as the number of qualified officers and analysts they have available, but over time, I think we are going to be getting more and more individuals with the requisite background

in intelligence and substantive expertise.

How do you incentivize these assignments and ensure that you get the quality of people that you need over time? Do you envision, for example, a terrorist-related intelligence challenge so enduring that we ought to develop a professional cadre for the Intelligence Community of terrorism analysts, perhaps even with a separate career service?

Well, a couple of points there. First of all, everyone who comes here is an assignee from his or her home agency, not a detailee. That's an important distinction because they bring with them their authorities from their parent organization. I believe that the terrorism threat to US interests is going to be an enduring one, and we need to have a sustained and very robust capability in the terrorism arena in order to deal with it. I think that TTIC is the first step toward having a real collaborative and integrated environment for analysts. And if we are going to do it well, we really are going to have to make some adjustments as far as the Intelligence Community's personnel system. We need to make sure there is recognition that service within TTIC is looked upon as a career enhanc-

ing assignment, just as a tour of duty in a "joint assignment" is seen as a prestige factor for career development in the military. We are right now completing the negotiation of MOAs with all of the partner agencies regarding what the personnel obligations are. These will include commitments from those agencies that service in TTIC will be appropriately recognized and that those individuals will serve in TTIC for a minimum of two years.

Are we moving toward a time when "counterterrorism analysts" will represent a distinct professional career track, analogous to economic analysts, political analysts, and military analysts?

I think terrorism analysis is rather unique and really requires some well-developed skills. And so I very much see it as a distinct discipline within the intelligence arena. I believe that an analyst can serve his or her entire career working on terrorism. I would encourage them, as I would any analyst, to spend time outside of their specific field of interest, because it really helps to put their area of expertise in some kind of context and perspective. But I fully expect that younger analysts who are either in TTIC or in one of our partner agencies, if they're committed to being terrorism analysts, are going to find ample opportunity for a 20- or 30-year career to serve in support of specific and discrete missions related to terrorism.

66

Within the walls of TTIC, there has been a tremendous blending together of the different [organizational] cultures.

99

As an Intelligence Community, we need to think through what the career tracks should look like so that analysts have a variety of attractive options. They shouldn't see themselves as on a conveyor belt moving up within a single stovepipe. One of the great things about TTIC is that you have analysts from the Secret Service, the Coast Guard, CIA, DIA, FBI, whatever, sitting next to each other and really understanding what other government organizations do and seeing the importance of terrorism analysis for those agencies and missions. This has opened up the horizons, not just in terms of what the requirements are, but what the possibilities are as far as their involvement in some of these areas. So, for anybody who really wants a career on terrorism, there is going to be no dearth of opportunities and positions.

In recent discussions about intelligence transformation, a prominent theme is the need to break down old organizational barriers, promote horizontal integration, and intensify collaboration. It's often said that one of the immediate challenges that goes along with this is understanding and minimizing the effects of "culture clash," when employees from a wide variety of organizations are brought together. What are your impressions of how that has worked? Has "culture clash" manifested itself in ways that were unexpected or require some work to overcome?

It's interesting. People ask how we have been able to deal with all these representatives from these different agencies being put in this cultural cauldron. To be quite frank, we never really had to work at trying to develop a TTIC culture. When you bring together analysts, information systems, and databases, and when you have a critically important mission, individuals quickly forget whether they are from CIA or DIA or Secret Service. They work together because the mission is so important. What they are here to do is to understand the terrorist threat and to prevent future 9/11s. And so we found an immediate bonding among the analysts here.

Quite honestly, some clashes arise when we deal with some of the partner agencies, because some individuals look upon TTIC as a competitive organization. I think they need to view us as a part of them and they a part of us. But within the walls of TTIC here, we find that there has been a tremendous blending together of the different cultures in an enriching sense, because they better understand what the others' missions are. I think a lot of the cultural clashes that take place are the

result of ignorance, because an analyst or an individual officer from one agency really doesn't understand or appreciate what the mission requirements are of another department or agency. If they become intimately familiar with those missions then they say, "Oh, I understand," and a lot of those barriers quickly break down. That's why I'm a strong proponent of an overhaul of the Intelligence Community, because we have grown up within stovepipes, which have been detrimental to the overall intent of the Intelligence Community.

Do you regard TTIC's organization and practices as a model for the way Intelligence Community components should operate in the future?

TTIC is so new and innovative, and I really believe that it is the shape of things to come in the future. We should not still be operating in the 1947 mindset of capabilities-based organizations that pursue related objectives and initiatives separately. What we need to do is to make sure that we establish centers like TTIC, where the capabilities of CIA, DIA, and NSA, as well as of some of the newer players on the intelligence field—such as the Department of Homeland Security and the FBI—are fused together in an integrated environment.

That's why the concept of a Director of National Intelligence is an appealing one because it moves the Intelligence Commu-

nity away from being focused solely on "foreign intelligence," which has been the case for the past 55 years or so. Intelligence is more than foreign intelligence; it is domestic intelligence as well. And there really needs to be better orchestration of the overall intelligence effort across the community.

Let me ask about analytic redundancy. There's a limited pool of experienced counterterrorism analysts and so how they're concentrated and distributed makes a difference. Given the limited talent pool, you've got to think carefully about how much competing analysis makes sense. And today, your mandate is shared in whole or in part by DHS's Information Analysis and Information Protection Directorate, by FBI's Counterterrorism Division and Office of Intelligence, by OTA and CIA, and by DIA's Joint Intelligence Task Force-Counterterrorism (JITF-CT). Could you describe the types of analytic tasks uniquely performed at TTIC and explain how they differ from those being performed at other CT centers around town?

Well, there are a couple of issues here. First of all, with the standup of the Department of Homeland Security and with the Office of Intelligence of the FBI, there was strong interest in the White House and elsewhere that we have the ability to integrate terrorism information and related analysis, so you don't have separate information and
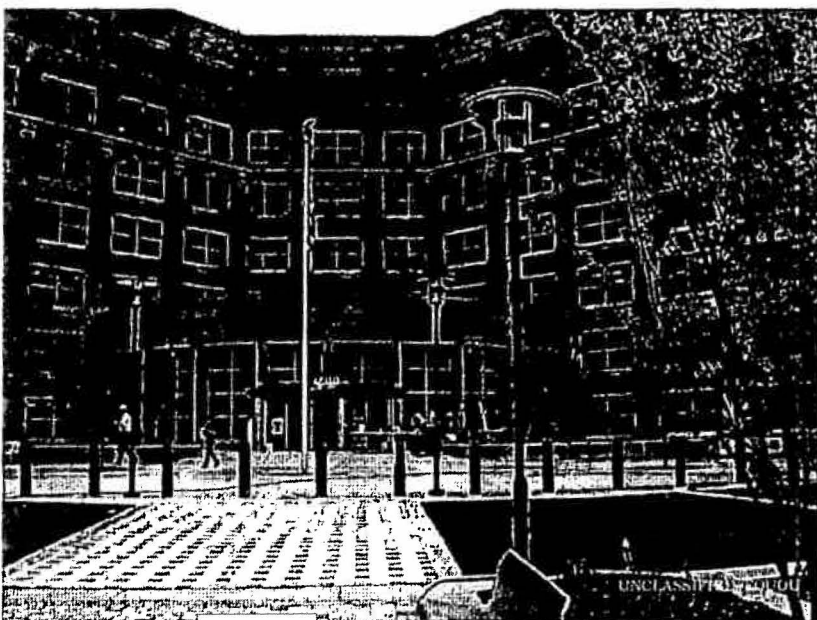
TTIC Headquarters.

analysis streams going to senior officials and others. TTIC now has the responsibility to provide integrated assessments of the terrorist threat; for example, when there are Principals Committee meetings or Deputies Committee meetings or the president needs to be briefed on something about the terrorist threat, TTIC represents the views from throughout the community and provides an integrated, fused assessment identifying differing views within the community as appropriate. So that is sort of a unique responsibility that we have on behalf of those partner agencies.

But getting to your point about competitive or redundant analysis, one of the real concerns that I have is that there needs to be

better orchestration of the different analytic elements that exist within the federal government because as you point out, analytic resources are finite. We cannot waste the time or talent of any analyst by doing unnecessarily redundant work. I still see unnecessary—and unhelpful—redundancy when there is a terrorist incident or threat, and a half a dozen or more analytic entities produce very similar products. When we do that, we are wasting those precious resources, because we are not covering the universe of terrorism issues appropriately. TTIC has been trying to promote the idea of a national framework that has a rational allocation of responsibilities so we don't have that unnecessary duplication. Clearly, some redundancy and

CUJ6L.ọ5Ü7

> **66**
>
> **We need thoughtful and intentional competitive analysis—not haphazard redundancy.**
>
> **99**

alternative analysis is desirable—indeed, essential—but there needs to be a common game plan and not just a free market analytic environment out there.

At times, unfortunately, I would equate the situation to what happens in soccer played by seven-year-olds: When the ball goes to one end of the field, all those little feet scurry to that side of the field, leaving the rest of the field unattended. We cannot afford to do that on terrorism analysis in the US government. We need thoughtful and intentional competitive analysis—not haphazard redundancy. We need to make sure that every part of the field is covered 24 hours of the day, and that requires overall orchestration. In this manner, the "orchestrator" knows exactly what TTIC is doing, and what CIA, FBI, DHS, and others are doing, and he or she can make informed decisions about adjusting areas of analytic emphasis.

Your remarks suggest to me that TTIC should emerge as the US government's unquestioned, authoritative center of gravity for CT analysis. This would leave the important departmental intelligence components to focus on their unique responsibilities for packaging, presenting, and communicating information in a way that is most responsive to their leadership. With such an arrangement, it becomes tougher to argue for maintaining a truly robust counterterrorism analytic capa-

bility in CIA's Office of Terrorism Analysis.

I agree with you completely on the need for the TTIC—or an eventual National Counterterrorism Center—to be the "center of gravity" for terrorism analysis. That center of gravity you refer to, and I use that same term myself, is a place where the shared statutory responsibilities of those partner agencies can be fulfilled in an integrated, collaborative environment. And if you look at the statutory language that set up the CIA, and you look at the Homeland Security Act, and you look at other statutes and commissioning documents that have given these departments and agencies responsibility for assessing and analyzing the terrorist threat, you can understand why same types of things are being done in different places. Those statutory responsibilities, however, can be fulfilled in this collective joint venture known as TTIC on behalf of all those departments and agencies.

There are discreet mission responsibilities that can and must be fulfilled inside of those agencies themselves. For example, DHS has tremendous responsibility for understanding the vulnerabilities of the US home-

land—what opportunities at the state or local level could terrorist groups take advantage of; what are the materials, the venues, the security weaknesses, and lapses? These are the things that DHS is uniquely able to address. But the task of analyzing the nature and scope of the threat that is coming from the terrorist groups need not be done in DHS as well as in TTIC.

Also, I think you need a place within the US government where there is truly an independent and neutral assessment of the terrorist threat. Each of TTIC's partner agencies has a responsibility for actions related to the threat. DHS has responsibility for mitigating the threat, putting in place defensive measures, and making the homeland a more difficult place for terrorists to ply their trade. CIA has responsibility for helping to neutralize the threat and for collecting against it. FBI, from the law enforcement perspective, has the responsibility to find individuals here in country and overseas who are threatening US interests. While these agencies need internal analytic resources to guide their activities, operations, and investigations, I would argue that the assessments of the threat posed by terrorist groups should be done primarily by TTIC and, eventually, by a National Counterterrorism Center.

So would you then confine the role of departmental CT analysts and those in CTC to "direct support"—for example, targeting

> ## There are areas that are best addressed by the country and functional analysts in CIA who have tremendous breadth and depth of experience.

support to the Directorate of Operations?

Not exactly. There are also analytic responsibilities, I think, that need to remain within those individual agencies and departments. CIA analysts for example, will need to track, understand, and analyze the root causes of terrorism. Also, they need to address the political, economic, and social consequences of terrorism, as well as state sponsorship issues, and the counterterrorism policies and capabilities of foreign governments. These are areas that are best addressed by the country and functional analysts in CIA who have tremendous breadth and depth of experience on foreign intelligence issues. We shouldn't try to build that capability within TTIC when it already exists somewhere else. CIA is uniquely qualified to do that. Likewise, DHS is uniquely qualified to be doing the analysis on homeland vulnerabilities, while FBI analysts are uniquely qualified to address purely domestic intelligence matters.

Within TTIC, you have an Information Sharing and Knowledge Development Department, including an element that's charged with Advanced Analytic Techniques and Red Teaming. Can you tell us a bit about the types of advanced analytic techniques being explored and considered and perhaps as well a word about how your red teaming activities are being developed and deployed?

Well, it's one of the areas that we are still in the process of developing, but let me talk a little bit about it conceptually. We have unprecedented access to all these networks and all these databases—terabytes upon terabytes of data—but there's absolutely no way that we could put eyes on every bit of information even if we had thousands of analysts here. What we really need to do in an environment like TTIC that has this type of access to data, is to apply robust analytic tools, the computing power that's out there, so that we can make the connections between seemingly unrelated bits and pieces of information.

And there is tremendous analytic tool capability and tremendous computing power available to do this. We're not doing "data mining," but we're applying the analytic tools for sophisticated search queries against those different databases and information systems. And if you have individuals and databases from diverse organizations such as the Transportation Security Administration, Coast Guard, Secret Service, FBI, CIA, and others, you can do queries in ways that traditionally have not been done

in the foreign intelligence community. So what we are trying to do is to match the expertise, the backgrounds, and the skill areas of the people in this team with databases, computing power, and analytic tools. If you bring that together, you are able to leverage the knowledge of the individuals, the capability of technology, and the existence of data. We are going to be seeing new ways of surfacing connections between those dots and creating new knowledge, and that's what we mean by know-ledge development.

Another aspect of the analytic mission is guiding collection priorities and tasking. A coordinated US government strategy for collecting and exploiting intelligence across the domestic intelligence-foreign intelligence divide implies the need for an analytic center of gravity that directly supports and guides tasking. Can TTIC perform that function today?

Well, right now TTIC is the mission manager on terrorism for the community as far as the collection requirement system is concerned. We do play a lead role; we work with the other agencies and departments to determine the national intelligence priorities framework for terrorism. As you know, there is a very well-developed collection requirement system on foreign intelligence, and what we have been trying to do over the past year or so is to broaden that focus in the terrorism world, so it's not just foreign intelligence. For example, right now we are dealing with the

CO56_8307

SECRET/
TTIC

"

The National Intelligence Collection Board . . . is likely to expand to include domestic intelligence requirements.

"

threat to the homeland that al-Qa'ida poses, and so we've had a number of meetings where organizations that have focused traditionally on foreign intelligence get together with those departments and agencies that are now responsible for domestic intelligence collection and dissemination. As the Intelligence Community evolves over the next year or two, we are going to see continued changes so that, for example, the National Intelligence Collection Board, which has had a foreign intelligence focus, is likely to expand to include domestic intelligence requirements.

Information acquired at the local level in the US could be of high value to TTIC. For example, the local police department in a large Midwest city has an ongoing surveillance program aimed at potential terrorists who are affiliated with a local mosque. Some may be US citizens, others not. Local police have been monitoring their communications with other residents of the US suspected of terrorist ties. Can TTIC request or routinely receive a list of these names and the assessments or observations of that local police department, or are you receiving them now?

The FBI has the responsibility for working with local law enforcement as far as getting information that is relevant to the terrorist threat. The FBI, working with its federal, state, and local partners on the Joint Terrorism Task Force (JTTF), is putting in place a system that will facili-

tate the reporting and onward dissemination of information acquired by local law enforcement to the broader counterterrorism community. The FBI puts all that information into its databases and information systems, and TTIC has unfettered access to those FBI systems.

So it's a "pull system," in effect, for TTIC.

Right, data do not have to be pushed to us by the FBI or by other organizations. That's the great thing about TTIC, we don't have to rely on CIA or FBI or others to package up information and send it to us. We have full real-time visibility into their information systems and databases. So anything that's committed to an electron in the FBI system or the CIA system, we have real-time access to it.

One of the most difficult challenges has been access by others in the community to the databases of CIA's Directorate of Operations. The Homeland Security Act provides that DHS is to be given necessary and adequate accesses to all databases containing covered information. To your knowledge, do the legacy IT architectures, which are designed

mainly for vertical information flow, currently permit the kind of ready access to raw DO data by both TTIC and the Department of Homeland Security that's mandated by law?

Well, we at TTIC have full and unfettered access to DO information systems, DO cable traffic, and DO databases. DHS representatives here in TTIC have that type of access, so the obligation on the part of CIA and FBI to make even the most sensitive information available to DHS is being met. A lot of that is being fulfilled through the TTIC construct, and other types of avenues of information sharing have been created over the past year. So, we feel good here about the visibility that TTIC and the partner agencies have into those information systems. Now what we have to do, as I mentioned earlier, is apply those analytic tools against the databases so that we are able to surface relevant information.

If I understand correctly, you're saying it is the responsibility of DHS officers assigned to TTIC to determine whether data they have access to should be relayed to their colleagues back in their home agency of DHS.

It is correct up to a point. DHS analysts have visibility into the CIA and FBI databases and information systems, and if they see anything that is of relevance to the Department of Homeland Security that has not yet been formally disseminated, we have mechanisms in place that allow

8 SECRET

❝

What we don't want is to have everybody 'shotgunning' information to all the different constituencies.

❞

that analyst to go back to CIA or the FBI and say, "you may not realize this, but this information is important. It must be disseminated." We at TTIC do not disseminate raw intelligence. But it is our responsibility to make sure that if we identify something that is important, we then tell the originating agency, "You must get this out, you must disseminate this, it is important to others."

But we cannot allow individual officers to decide and then disseminate on their own what within that great mass of raw intelligence should go to other entities. It has to be done the right way; we take very seriously our obligations to protect sources and methods. We have been given visibility into the most sensitive information that the US government has available to it, and we have to make sure that we protect sources and methods and do the right thing as far as sharing that information.

You've touched already on the dissemination challenge and the important progress that's been made. Do TTIC responsibilities for dissemination of your products stop at the national level now, deferring to DHS or the FBI for further dissemination to state and local officials under certain circumstances?

Correct. When TTIC was stood up, it was decided that we would disseminate information directly only to our federal partners. And so we share information with DHS, FBI, DOD, and others.

DHS has the statutory responsibility and the primary responsibility for sharing information with state and local officials as well as the private sector. The FBI has a statutory responsibility to make sure that information is shared with law enforcement. So, what we do is provide information and analysis to DHS and FBI so that they can then share it as appropriate with their non-federal constituents.

This is part of the nascent national architecture for both horizontal and vertical information sharing. We need to be able to move information from the Top-Secret level of a federal department all the way to the Sensitive-But-Unclassified (SBU) level such that it is available to the cop on the street or the local mayor. But it has to be done in a coordinated and orchestrated fashion. What we don't want to do is to have everybody "shotgunning" information to all the different constituencies. We have to recognize roles and responsibilities, and DHS has a certain responsibility for forwarding that information down vertically, as does the FBI.

Suppose TTIC prepares a classified report on a likely foreign

terrorist threat to a private oil refinery in Texas. DHS wants to alert the affected private sector persons. Who makes the decision regarding the scope and nature of what DHS or the FBI can disseminate further? Is that determination made by DHS, or must the "data owners" or originator give prior approval?

I prefer the term "data stewards" to "data owners," because stewardship implies an obligation to fulfill the responsibilities of information sharing. Right now, to take your example, DHS would have to make sure that the data steward—for example, the CIA or FBI—is comfortable with the language being sent to a broader audience. In most cases today, there's no reason, from a technical or policy perspective, that even sensitive information acquired by CIA's foreign intelligence collection should not flow expeditiously from the point of origin to TTIC, DHS, and FBI, as well as to non-federal entities. And if it has to go down to the governor or the mayor or the local police chief, you can shape the information at the point of origination or put it into a format that is going to be usable at its endpoint that also protects sources and methods.

I would argue that CIA officers abroad need to send in a report that can be broken down automatically into two parts. One part contains the "who, what, where, when, and how" of an imminent terrorist attack, and that information goes quickly at the SBU level to all the appropri-

66

TTIC-like organizations are sprouting up worldwide.

99

ate end users. The other part of the report that provides the classified contextual information that's operationally sensitive and is not needed at the local level goes to a more restricted group of users. If the report has to go to the governor, mayor, or local police chief, there must be recognition at the point of origination that what's involved is the need to rapidly share actionable intelligence, and that means creating a format that makes information in the report "separable."

Right now, using your example, we see too many human interventions: a report comes in; a request is made for a releasable tear-line; it's then put into tear-line format; then it goes out to a federal consumer set at a classified level; and then that consumer will come back with a request to prepare it again at the SBU level for sharing with local law enforcement, and it has to go back to the originating agency to approve the language. There are too many steps here; it eats up time and resources. So we need to reengineer the system to make it more efficient from the get-go. That's why I emphasize so much the importance of coming to agreement on the overall business process architecture, to include greater clarity of information requirements based on agreed-upon roles and responsibilities.

Some of the analytic puzzles you work at the TTIC level may benefit from information first discovered by state or local authorities—for example, reports

of suspect behavior or casing activity at vulnerable sites. How well does the flow of information work in this direction, and who is responsible for ensuring local law enforcement knows what activities or behavior may have intelligence significance at TTIC?

You are absolutely right. It needs to be a two-way flow, from locals coming up as well as from federal officials going down, and all the way into the international environment. At this point, the FBI has the unique responsibility of ensuring that local law enforcement is kept informed of the terrorist threat and is provided requirements and information that will allow them to identify those things that are potentially terrorist related. DHS has a similar responsibility with respect to non-law enforcement officials at the state and local levels and leaders in the private sector. This is the direction in which the whole national architecture is evolving.

It is a very complex "system of systems" for ensuring education, information flow, and product dissemination systems across multiple domains within the US. And then you expand it into the international context, because we're really talking about an

international coalition against the terrorist threat. So it becomes an enormous challenge to integrate and knit together the different elements. Many have shared interests and responsibilities, but they frequently have very different mission responsibilities. This is obviously a daunting challenge and meeting it will take time.

Can you expand on the new challenges in the international context, particularly as they affect traditional intelligence liaison activities? Within the Intelligence Community, there is increased emphasis on horizontal integration to respond effectively. Liaison relationships, however, typically have been the province of vertically organized collection organizations. Can you, as the director of TTIC, interact seamlessly and efficiently with counterparts in other countries without being impeded by business practices that grew up around older organizational arrangements?

Well, TTIC isn't trying to take over the liaison responsibilities of these individual agencies. CIA and FBI will always maintain close, robust relationships with sister services overseas. But interestingly, other TTIC-like organizations are sprouting up worldwide. This reflects recognition that, with the very complexity of the challenge and the multitude of official entities involved in terrorism, national governments need a "portal," a place where you can plug these elements and information systems together. And so we

> ❝
>
> **The key to success involves harnessing the diverse capabilities from all elements of the US government.**
>
> ❞

have a very close relationship with our British counterpart, the Joint Terrorism Analysis Center. The Australians also have a TTIC-like structure, and other countries are moving down that road. The existence of these integrated, multi-agency national entities like TTIC makes for more effective international cooperation on terrorism than exclusive reliance on agency-to-agency connections.

Given the level of scrutiny and evaluation the Intelligence Community is receiving from so many quarters today, it is not surprising that radically different arrangements are being considered for managing and organizing intelligence. From the perspective of your unique mission, what would be the distinctive characteristics of a *transformed Intelligence Community?*

First and foremost, I would say better integration of effort. This is the key to success. It involves harnessing the diverse capabilities from all elements of the US government and applying them in an integrated way against priority national security issues. This will enhance both effectiveness and efficiency. A second desirable feature would be orchestration—clear leadership of a complex community. This is where the concept of a National Intelligence Director (NID) becomes attractive. It responds to the growing need for a well-coordinated effort, involving a vast array of capabilities applied against a very complex problem so that what emerges sounds more like a symphony than a cacophony. This orchestration of effort obviously is important not just for the foreign intelligence establishment, but extending to domestic intelligence as well. These are the main characteristics of the Intelligence Community I would like to see evolve.

John, thank you very much for your time today.
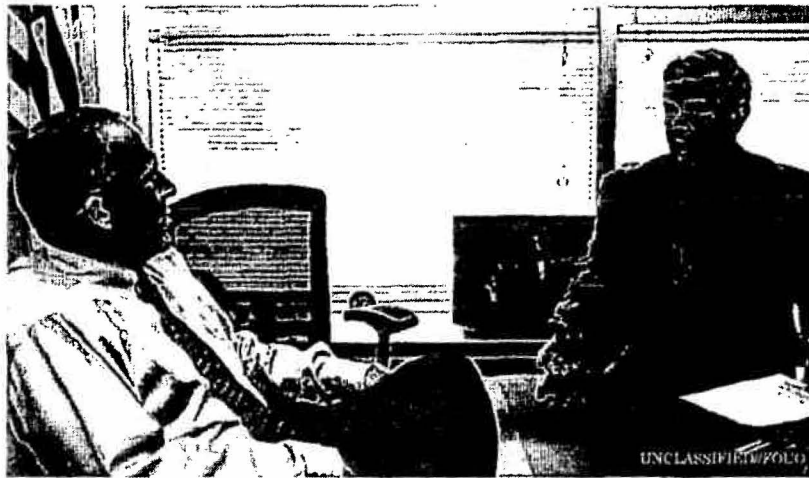
John Brennan with *Studies* Editorial Board Chairman